

SEALED

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

FILED

JUL 23 2019

CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY 8 DEPUTY

UNITED STATES OF AMERICA

v.

ROBERT WAYNE BOLING, JR. (1),
FREDRICK BROWN (2),
TRORICE CRAWFORD (3),
ALLAN ALBERT KERR (4), and
JONGMIN SEOK (5)

§ CRIMINAL NO.

§

§

§

§

§

§

§

§

§

§

§

§

§

§

§

§

§

§

SA 19 CR 0524 OG

SEALED
INDICTMENT

COUNT 1: 18 U.S.C. § 1349, Conspiracy
to Commit Wire Fraud

COUNTS 2-7: 18 U.S.C. § 1343 and 2,
Wire Fraud

COUNT 8: 18 U.S.C. § 1956, Conspiracy
to Commit Money Laundering

COUNTS 9-14: 18 U.S.C. § 1028A,
Aggravated Identity Theft

NOTICE OF GOVERNMENT'S
DEMAND FOR FORFEITURE

THE GRAND JURY CHARGES:

THE CONSPIRACY

At all times relevant herein:

OVERVIEW

1. Beginning in and around July 2014, and continuing through in or around July 2019, the Defendants, ROBERT WAYNE BOLING, JR. ("BOLING"), FREDRICK BROWN ("BROWN"), TRORICE CRAWFORD ("CRAWFORD"), ALLAN ALBERT KERR ("KERR"), and JONGMIN SEOK ("SEOK"), together with others known and

unknown to the Grand Jury, perpetrated a scheme to exploit stolen personal identifying information (“PII”) belonging to members of the United States military, including service members (active duty, reserve component, and National Guard) and veterans, their dependents, and civilians employed by the Department of Defense (collectively, “military-affiliated individuals”). The Defendants used the stolen PII to target military-affiliated individuals in various ways, such as stealing from military-affiliated individuals’ personal bank accounts and stealing pension and disability benefits paid to military-affiliated individuals by the Veterans Administration (“veterans benefits”). The Defendants then made financial transactions involving numerous bank accounts and money remittances to conceal and dispose of stolen monies.

2. Over the course of the scheme, the Defendants stole and exploited the PII of thousands of military-affiliated individuals and caused millions of dollars of actual and attempted losses to military-affiliated individuals, the Veterans Administration, and banks and credit unions across the United States.

3. The Defendants generally played the following roles in the scheme:

- a. **BOLING** was the principal orchestrator of the scheme. **BOLING** received stolen PII, and coordinated with and directed other Defendants and others to exploit the stolen PII in order to compromise military-affiliated individuals’ bank accounts, steal military-affiliated individuals’ veterans benefits, and remit stolen funds to the Philippines. **BOLING**, an American citizen raised in South Korea as a United States military dependent, lived in Angeles City, Philippines.
- b. **BROWN** was the primary source of stolen PII. From December 2010 through September 2015, **BROWN** had worked as a civilian medical records technician at the 65th Medical Brigade, United States Army, at Yongsan Garrison, South Korea.

In that capacity, **BROWN** had access to a substantial volume of military-affiliated individuals' PII, which he copied and transmitted to **BOLING**.

- c. **CRAWFORD** acted as a recruiter and supervisor of individuals who provided their bank accounts to be used to receive stolen funds ("money mules").

CRAWFORD, an American citizen living in the vicinity of San Diego, California, coordinated with **BOLING** to transfer funds stolen from military-affiliated individuals to be deposited into money mules' accounts. **CRAWFORD** also assisted in remitting stolen funds from money mules' accounts to members of the conspiracy in the Philippines.

- d. **KERR** and **SEOK** assisted **BOLING** in using military-affiliated individuals' PII to obtain additional records of military-affiliated individuals to facilitate the scheme, such as credit reports and official military personnel files. Like **BOLING**, **KERR** (an Australian citizen) and **SEOK** (a South Korean citizen) lived in Angeles City, Philippines (collectively, the Philippines Defendants).

OBJECT OF THE CONSPIRACY

4. The object of the conspiracy was to enrich the Defendants by stealing money and property from military-affiliated individuals, government-benefit programs, and financial institutions by means of identity theft, fraud, and money laundering.

MANNER AND MEANS OF THE CONSPIRACY

5. The scheme and artifice to defraud was carried out in the manner and means described below.

Theft of Military-Affiliated Individuals' PII

6. From in and around December 2010 through in and around September 2015, while employed as a medical records technician at Yongsan Garrison, **BROWN** worked with a database called the Armed Forces Health Longitudinal Technology Application ("AHLTA"), which is one of the United States military's principal repositories for electronic health records of military-affiliated individuals. As a medical records technician, **BROWN** had access to substantial volumes of military-affiliated individuals' PII. Specifically, beyond health-related data, AHLTA contained each military-affiliated individual's name, social security number, Department of Defense ID number (a unique 10-digit number assigned to military-affiliated individuals), date of birth, gender, mailing address, and telephone number. AHLTA was designed in such a way that the user could view the PII for approximately ten different military-affiliated individuals simultaneously.

7. While employed at the 65th Medical Brigade, **BROWN** took digital photographs of thousands of military-affiliated individuals' PII displayed in AHLTA in groups of ten. **BROWN** conveyed these photographs to **BOLING** through various communication channels. **BOLING** knew that **BROWN** was taking photographs of his AHLTA computer screen in order to obtain military-affiliated individuals' PII, at one point asking **BROWN** whether or not **BROWN** had gotten "popped red handed snappin shots at the gig."

Exploitation of Military-Affiliated Individuals' PII

DS Logon

8. One of the principal means by which the Defendants exploited the stolen PII to commit identity theft was the compromise of military-affiliated individuals' Department of Defense Self-Service Logon ("DS Logon") accounts. DS Logon was a system that allowed

military-affiliated individuals access to more than 70 nonpublic websites using a single username and password. DS Logon was maintained by the Defense Manpower Data Center, the Department of Defense component agency responsible for maintaining data on U.S. military personnel. With a DS Logon account, a military-affiliated individual could access websites containing extensive personal and financial data, including PII for all of a military-affiliated individual's dependents (spouse and children), tax information, and health records, among other information. The user of a DS Logon account could also alter the account and routing numbers for bank accounts into which salaries, benefits, disability payments, and pensions were paid by the Department of Defense or the Veterans Administration. Without a DS Logon account, access to these websites required authentication using a common access card ("CAC"), a physical plastic card with an electronic chip in it that must be inserted into a keyboard or other device specifically designed to read it, or an in-person visit to a Department of Defense personnel office.

9. Creation of a DS Logon account required a user to visit a website maintained by the Defense Manpower Data Center and to input certain elements of a military-affiliated individual's PII. The user was also required to answer security questions based on entries in the military-affiliated individual's credit report. Correct responses to the security questions enabled the user to create a DS Logon account. This identity verification within the DS Logon system without the use of a CAC or an in-person visit to a Department of Defense personnel office was called "remote proofing." The DS Logon system also permitted identity verification via remote proofing for existing DS Logon accounts. A user could reset the username and password associated with an existing account by answering security questions to establish new credentials. Once a new password was established and the user had gained access to the DS Logon account,

the user could change the contact information the system used to notify the user of subsequent changes to the account.

10. Over the course of the scheme, the Defendants used the photographs of the AHLTA screens taken by **BROWN**, containing PII of thousands of military-affiliated individuals in the manner described above, to create and compromise DS Logon accounts.

eBenefits

11. One of the partner sites that could be accessed using a DS Logon credential was “eBenefits,” a web portal hosted by the Veterans Administration within the Western District of Texas. The servers through which all online communication with eBenefits flowed, and the administrative staff that supported the website, were physically located within the Western District of Texas. The eBenefits web portal provided military-affiliated individuals the ability to manage their Veterans Administration and Department of Defense benefits, claims, and military documents online.

12. The Defendants accessed eBenefits in furtherance of two related types of fraud against military-affiliated individuals.

a. Theft of Funds from Military-Affiliated Individuals’ Personal Bank Accounts:

Once logged into a military-affiliated individual’s DS Logon account, the Defendants accessed eBenefits in that military-affiliated individual’s name to obtain the account and routing number of the bank account into which the military-affiliated individual received veterans benefits. The Defendants then used that account and routing number combination, along with other PII, to steal money from the military-affiliated individual’s personal bank account. In some

instances, the Defendants contacted banks and other financial institutions by telephone, chat, and e-mail, and posed as military-affiliated individuals.

b. *Theft of Veterans Benefits:*

The Defendants also accessed eBenefits to substitute a bank account they controlled for the military-affiliated individual's own bank account, so that any veterans benefit would be paid directly to the Defendants.

Military-Focused Financial Institutions

13. The Defendants also used means other than eBenefits to steal from military-affiliated individuals, targeting personal bank accounts held through certain financial institutions with a significant military clientele. At least two such military-focused financial institutions, United States Automobile Association ("USAA") and Randolph-Brooks Federal Credit Union ("Randolph-Brooks FCU"), were based within the Western District of Texas, in the vicinity of San Antonio. By exploiting military-affiliated individuals' PII stolen by **BROWN**, and obtained through eBenefits and elsewhere, the Defendants caused millions of dollars in actual and attempted losses to military-affiliated individuals from those individuals' bank accounts held through military-focused financial institutions across the United States.

International Money Remittances

14. The Philippines Defendants, **BOLING**, **KERR**, and **SEOK**, worked with a network of "money mules" – co-conspirators who provided bank accounts into which stolen funds could be deposited. The money mules tended to operate from various locations within the United States, including San Antonio, within the Western District of Texas. **CRAWFORD** supervised several of these money mules, and, on several occasions, **CRAWFORD** accompanied the money mules to various bank branches in the vicinity of San Diego, California,

and directed the money mules to withdraw funds deposited into their bank accounts by the Philippines Defendants. **CRAWFORD** provided **BOLING** with the money mules' bank account information, and **BOLING** transferred funds stolen from military-affiliated individuals into the money mules' accounts. **CRAWFORD** then kept a percentage of the withdrawn funds and oversaw the transmittal of the remainder by means of international money services businesses to recipients in the Philippines, including the Philippines Defendants themselves as well as other parties whose names **BOLING** provided to **CRAWFORD**.

Example Acts in Furtherance of the Scheme

15. Over the course of the conspiracy, the Defendants exploited thousands of military-affiliated individuals' PII. The Defendants often targeted older military-affiliated individuals, who were less likely to use DS Logon and eBenefits, and disabled veterans, who were more likely to receive larger veterans benefits. The following examples of acts in furtherance of the scheme were typical of those engaged in by the Defendants.

a. Colonel H.C., United States Air Force

- i. At some point prior to May 2015, the exact date being unknown to the Grand Jury, **BROWN** provided **BOLING** with the PII of at least 50 military-affiliated individuals who all had the same last name, a relatively uncommon three-letter name beginning with the letter C.
- ii. On or about May 14, 2015, **BOLING** used the PII of Colonel ("Col.") H.C., one of those 50 individuals with the same three-letter last name, to effectuate a wire transfer in the amount of \$16,250 from Col. H.C.'s USAA bank account to a Wells Fargo bank account in the name of G.H., a money mule.

- iii. That same day, **BOLING** provided the following instructions to a member of the conspiracy:

From usaa bank of [H.C.] in...GA. Tell him take out 14 or 15 k...I just need 7000 even....

Tell him to have a good story... Just tell him to say its his uncle sending money for his family or some shit but not too much detail....

...In fact i have a perfect idea... Send me 3000 all at once asap and then send 2000 to Fredrick Brown in Western Union... Please confirm so i can tell Fred.

- iv. On or about May 18, 2015, after the funds had been transferred to the account of G.H., **BOLING** expressed concern to **BROWN** that G.H. was delayed in remitting the funds stolen from Col. H.C. **BOLING** then asked **BROWN** for additional information on G.H. (also a U.S. military dependent) and G.H.'s family, for the purpose of threatening G.H.'s family members if G.H. did not send the funds promptly. In response, **BROWN** then queried G.H.'s electronic health record in AHLTA, which included information on G.H.'s family. Shortly thereafter, G.H. then sent a portion of the money stolen from Col. H.C.'s account to the Philippines as directed by **BOLING**.

b. Petty Officer First Class A.D., United States Navy

- i. On or about October 19, 2016, a member of the conspiracy based in the Philippines conducted initial registration of the eBenefits account of Petty Officer First Class ("PO1") A.D., and thereby obtained the account and

routing information of the account held through Kitsap Federal Credit Union (“Kitsap FCU”) into which PO1 A.D.’s veterans benefit was paid.

- ii. On that date in October 2016, PO1 A.D. was 79 years old, and had never used DS Logon or eBenefits.
- iii. On or about October 24, 2016, **BOLING** contacted Kitsap FCU customer service, and impersonated PO1 A.D.
- iv. Over the course of the following two days, **BOLING** arranged two wire transfers out of the bank account of PO1 A.D. The first wire transfer, in the amount of \$18,500, was successfully deposited into the bank account of a member of the conspiracy. Following that transfer, PO1 A.D. contacted Kitsap FCU customer service, and advised that the wire had been unauthorized. **BOLING** then attempted a second wire transfer in the amount of \$27,000 from PO1 A.D.’s account, which was denied as unauthorized. Kitsap FCU then closed PO1 A.D.’s account, and assigned PO1 A.D. a new Kitsap FCU account number.
- v. On or about November 18, 2016, **SEOK** accessed the eBenefits account of PO1 A.D. **SEOK** took screen captures from within PO1 A.D.’s eBenefits account, capturing his PII, including PO1 A.D.’s Veterans Administration file number, and the account and routing number for PO1 A.D.’s new Kitsap FCU account after the unauthorized wires orchestrated by **BOLING** in October 2016.
- vi. On or about December 15, 2016, a member of the conspiracy accessed PO1 A.D.’s eBenefits account and substituted a Community Federal

Savings Bank account and routing number in place of the Kitsap FCU account details on file with the Veterans Administration.

- vii. On or about December 20, 2016, PO1 A.D.'s veterans benefit, in the amount of \$1,451.71, was paid to the Community Federal Savings Bank account, instead of PO1 A.D.'s own account.

c. Major R.W., United States Army

- i. On or about March 6, 2017, **BOLING** accessed the DS Logon account of Major ("Maj.") R.W., and e-mailed a screenshot to **SEOK** of Maj. R.W.'s profile screen from within DS Logon.
- ii. On that date in March 2017, Maj. R.W. was 76 years old. Maj. R.W. was a 100% service-connected disabled veteran, and had been a prisoner of war.
- iii. Approximately 20 minutes later, **SEOK** accessed Maj. R.W.'s eBenefits account. **SEOK** then e-mailed **BOLING** photographs of **SEOK**'s laptop screen showing the profile page for Maj. R.W.'s eBenefits account. The subject line of the e-mail from **SEOK** to **BOLING** read "Have Big money. may be.."
- iv. Approximately 10 minutes later, **SEOK** conveyed to **BOLING** certain details about Maj. R.W.'s veteran status, including Maj. R.W.'s disability benefit amount, the USAA bank account and routing numbers into which his disability benefit was being paid, and a screenshot from within eBenefits showing a list of Maj. R.W.'s service-connected disabilities.

- v. On or about April 16, 2017, a member of the conspiracy accessed Maj. R.W.'s eBenefits account and removed Maj. R.W.'s USAA bank account and routing information, substituting account and routing information of an American Express debit card account.
- vi. On or about April 19, 2017, Maj. R.W.'s monthly veterans benefit, in the amount of \$2,915.55, was paid into the American Express debit card account, instead of Maj. R.W.'s USAA bank account.

d. Col. F.C., United States Air Force

- i. On or about March 9, 2017, **SEOK** accessed both the DS Logon and eBenefits accounts of Col. F.C., who had the same three-letter last name as Col. H.C. (referenced above in paragraph 15a), and was also one of the approximately 50 individuals whose PII **BROWN** provided to **BOLING** no later than May 2015.
- ii. On that date in March 2017, Col. F.C. was 66 years old.
- iii. That same day, **SEOK** e-mailed to **BOLING** certain PII of Col. F.C. obtained from eBenefits, including the account and routing number of the Pentagon Federal Credit Union ("Pentagon FCU") account into which Col. F.C. received a veterans benefit. The subject line of the e-mail was "Pentagon."
- iv. Approximately one minute later, **BOLING** forwarded **SEOK**'s e-mail, including Col. F.C.'s PII and the subject line "Pentagon," to **KERR**.
- v. On or about March 28, 2017, a member of the conspiracy accessed Col. F.C.'s Pentagon FCU account online and took out a \$2,000 loan, which

was deposited to Col. F.C.'s checking account. At that time, Pentagon FCU identified the transaction as fraudulent and closed Col. F.C.'s account.

e. Chief Petty Officer L.W., United States Navy

- i. On or about October 10, 2017, **KERR** accessed the eBenefits account of Chief Petty Officer ("CPO") L.W.
- ii. That same day, **KERR** conveyed to **BOLING** certain PII of CPO L.W., including a credit report as well as the Navy Federal Credit Union ("Navy FCU") bank account and routing information of the account into which CPO L.W.'s monthly veterans benefit was paid and the contact telephone number on file with the Veterans Administration for CPO L.W.
- iii. On or about December 9, 2017, a member of the conspiracy called the customer service line of Navy FCU and impersonated CPO L.W., using call-spoofing technology to appear to be calling from the number on file with the Veterans Administration for CPO L.W. The caller was unable to answer all of the security questions posed by the customer service representative, and terminated the call without completing any transactions.

f. Master Sergeant E.R., United States Air Force

- i. On or about June 18, 2018, **BOLING** contacted **CRAWFORD** and arranged for a wire transfer from the Randolph-Brooks FCU account of Master Sergeant ("MSgt") E.R. **CRAWFORD** provided the name of D.B., a money mule, along with details of a Wells Fargo account in the

name of D.B., including the account and routing number, online banking username and password, and the contact information linked to D.B.'s account.

- ii. On that date in June 2018, E.R. was 73 years told, and a resident of New Braunfels, in the vicinity of San Antonio, Texas and within the Western District of Texas.
- iii. In response, the following day, **BOLING** wrote to **CRAWFORD** "The request sent...we on standby...\$9,600 from randolph brooks Credit union...Senders name I sent [E.R.] Jr. From Texas." **CRAWFORD** responded "...they keep say 24 hour wait the money there they said . everything good but 24 hour hold." **BOLING** replied "Yeah it should be all good tomorrow... they used to do that shit to us always... just don't lose your boy by tomorrow."
- iv. That day, \$9,600 was wired from MSgt E.R.'s account to D.B.'s account.
- v. Between on or about June 19, 2018, and on or about June 27, 2018, **BOLING** arranged for a total of five wires, each between \$7,300 and \$9,600, to be sent from MSgt E.R.'s account to the account of D.B., for a total of \$41,500. D.B., under **CRAWFORD**'s supervision, withdrew funds from D.B.'s account shortly after each wire transfer and, by on or about June 27, 2018, D.B. had withdrawn the entire sum of \$41,500 from D.B.'s account.

COUNT ONE
Conspiracy to Commit Wire Fraud
[18 U.S.C. § 1349]

16. Count One incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

17. Beginning sometime in 2014, the exact date being unknown, and continuing until the date of this Indictment, in the Western District of Texas and elsewhere, the Defendants,

ROBERT WAYNE BOLING, JR. (1),
FREDRICK BROWN (2),
TRORICE CRAWFORD (3),
ALLAN ALBERT KERR (4), and
JONGMIN SEOK (5)

did knowingly and intentionally conspire and agree with others known and unknown to the Grand Jury to commit certain offenses against the United States, namely: Wire Fraud, in violation of 18 U.S.C. § 1343, that is, knowingly and with intent to defraud, having devised and having intended to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, in this case, a fraudulent scheme to steal from military-affiliated individuals, for the purpose of executing the scheme and artifice, transmitted and caused to be transmitted by means of wire, radio and television communication in interstate commerce certain writings, signs, signals, pictures and sounds.

All in violation of Title 18, United States Code, Section 1349.

COUNTS TWO THROUGH SEVEN**Wire Fraud****[18 U.S.C. §§ 1343 and 2]**

18. Counts Two through Seven incorporate by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

19. On or about the following dates, in the Western District of Texas and elsewhere, the Defendants, aiding and abetting each other, knowingly and with intent to defraud, having devised and having intended to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, in this case, a fraudulent scheme to steal from military-affiliated individuals, for the purpose of executing the scheme and artifice, transmitted and caused to be transmitted by means of wire, radio and television communication in interstate commerce certain writings, signs, signals, pictures and sounds to and from the Western District of Texas, as described below:

COUNT	DATE	DEFENDANTS	DESCRIPTION
2	May 14, 2015	ROBERT WAYNE BOLING, JR. (1), FREDRICK BROWN (2)	Wire transfer from the USAA bank account of victim H.C.
3	October 19, 2016	ROBERT WAYNE BOLING, JR. (1), JONGMIN SEOK (5)	Access to eBenefits account of victim A.D.
4	March 6, 2017	ROBERT WAYNE BOLING, JR. (1), JONGMIN SEOK (5)	Access to eBenefits account of victim R.W.
5	March 9, 2017	ROBERT WAYNE BOLING, JR. (1), FREDRICK BROWN (2), ALLAN ALBERT KERR (4), JONGMIN SEOK (5)	Access to eBenefits account of victim F.C.
6	October 10, 2017	ROBERT WAYNE BOLING, JR. (1), ALLAN ALBERT KERR (4)	Access to eBenefits account of victim L.W.

7	June 18, 2018	ROBERT WAYNE BOLING, JR. (1), TRORICE CRAWFORD (3)	Wire from the Randolph-Brooks FCU account of victim E.R.
---	---------------	---	---

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT EIGHT

**Conspiracy to Commit Money Laundering
[18 U.S.C. § 1956(h)]**

20. Count Eight incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

21. Beginning sometime in 2014, the exact date being unknown, and continuing until the date of this Indictment, in the Western District of Texas and elsewhere, the Defendants,

**ROBERT WAYNE BOLING, JR. (1),
FREDRICK BROWN (2),
TRORICE CRAWFORD (3),
ALLAN ALBERT KERR (4), and
JONGMIN SEOK (5)**

did knowingly combine, conspire, and agree with other persons known and unknown to the Grand Jury to commit offenses against the United States in violation of Title 18, United States Code, Section 1956, namely: to knowingly conduct and attempt to conduct financial transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, Wire Fraud in violation of 18 U.S.C. § 1343, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

All in violation of Title 18, United States Code, Section 1956(h).

COUNT NINE
Aggravated Identity Theft
[18 U.S.C. § 1028A]

22. Count Nine incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

23. On or about May 14, 2015, in the Western District of Texas and elsewhere, the Defendants,

ROBERT WAYNE BOLING, JR. (1), and
FREDRICK BROWN (2)

did knowingly use, and aid, abet, induce, and procure the use of, without lawful authority, a means of identification of another person, to wit, a name, date of birth, and social security number, belonging to H.C., during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), namely Conspiracy to Commit Wire Fraud, as charged in Count One of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

COUNT TEN
Aggravated Identity Theft
[18 U.S.C. § 1028A]

24. Count Ten incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

25. Between on or about October 19, 2016 and December 20, 2016, in the Western District of Texas and elsewhere, the Defendants,

ROBERT WAYNE BOLING, JR. (1), and
JONGMIN SEOK (5)

did knowingly use, and aid, abet, induce, and procure the use of, without lawful authority, a means of identification of another person, to wit, a name, bank account number, and Veterans Administration file number, belonging to A.D., during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), namely Conspiracy to Commit Wire Fraud, as charged in Count One of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

COUNT ELEVEN
Aggravated Identity Theft
[18 U.S.C. § 1028A]

26. Count Eleven incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

27. On or about March 6, 2017, in the Western District of Texas and elsewhere, the Defendants,

ROBERT WAYNE BOLING, JR. (1), and
JONGMIN SEOK (5)

did knowingly use, and aid, abet, induce, and procure the use of, without lawful authority, a means of identification of another person, to wit, a name, date of birth, social security number, and Department of Defense identification number, belonging to R.W, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), namely Conspiracy to Commit Wire Fraud, as charged in Count One of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

COUNT TWELVE
Aggravated Identity Theft
[18 U.S.C. § 1028A]

28. Count Twelve incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

29. On or about March 9, 2017, in the Western District of Texas and elsewhere, the Defendants,

ROBERT WAYNE BOLING, JR. (1),
FREDRICK BROWN (2),
ALLAN ALBERT KERR (4), and
JONGMIN SEOK (5)

did knowingly use, and aid, abet, induce, and procure the use of, without lawful authority, a means of identification of another person, to wit, a name, date of birth, social security number, and Department of Defense identification number, belonging to F.C., during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), namely Conspiracy to Commit Wire Fraud, as charged in Count One of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

COUNT THIRTEEN
Aggravated Identity Theft
[18 U.S.C. § 1028A]

30. Count Thirteen incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

31. On or about October 10, 2017, in the Western District of Texas and elsewhere, the Defendants,

**ROBERT WAYNE BOLING, JR. (1), and
ALLAN ALBERT KERR (4)**

did knowingly use, and aid, abet, induce, and procure the use of, without lawful authority, a means of identification of another person, to wit, a name, date of birth, social security number, and Veterans Administration file number, belonging to L.W., during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), namely Conspiracy to Commit Wire Fraud, as charged in Count One of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

**COUNT FOURTEEN
Aggravated Identity Theft
[18 U.S.C. § 1028A]**

32. Count Fourteen incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

33. On or about June 18, 2018, in the Western District of Texas and elsewhere, the Defendants,

**ROBERT WAYNE BOLING, JR. (1), and
TRORICE CRAWFORD (3)**

did knowingly use, and aid, abet, induce, and procure the use of, without lawful authority, a means of identification of another person, to wit, a name and bank account number belonging to E.R., during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), namely Conspiracy to Commit Wire Fraud, as charged in Count One of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

NOTICE OF GOVERNMENT'S DEMAND FOR FORFEITURE

I. Forfeiture Statutes for Fraud and Conspiracy
[18 U.S.C. § 981(a)(1)(C), as made applicable by 28 U.S.C. § 2461(c)]

As a result of the foregoing criminal violations set forth in Counts One through Seven, the United States gives notice that it intends to forfeit, but is not limited to, the property listed below from Defendants **ROBERT WAYNE BOLING, JR., JR. (1), FREDRICK BROWN (2), TRORICE CRAWFORD (3), ALLAN ALBERT KERR (4), and JONGMIN SEOK (5)**. The Defendants shall forfeit all right, title, and interest in said property to the United States pursuant to FED. R. CRIM. P. 32.2 and 18 U.S.C. § 981(a)(1)(C), which is made applicable to criminal forfeiture by 28 U.S.C. § 2461(c). In pertinent part, Section 981 provides:

18 U.S.C. § 981. Civil Forfeiture

(a)(1) The following property is subject to forfeiture to the United States:

* * *

(C) Any property, real or personal, which constitutes or is derived from proceeds traceable to . . . any offense constituting "specified unlawful activity" (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense.

Wire Fraud is an offense constituting "specified unlawful activity" as defined in section 1956(c)(7) of this title.

II. Forfeiture Statute for Money Laundering

[18 U.S.C. § 982(a)(1)]

As a result of the foregoing criminal violations set forth in Count Eight, the United States gives notice that it intends to forfeit, but is not limited to, the property listed below from Defendants **ROBERT WAYNE BOLING, JR. (1), FREDRICK BROWN (2), TRORICE CRAWFORD (3), ALLAN ALBERT KERR (4), and JONGMIN SEOK (5)**. The Defendants shall forfeit all right, title, and interest in said property to the United States pursuant to FED. R. CRIM. P. 32.2 and 18 U.S.C. § 982(a)(1), which states:

18 U.S.C. § 982. Criminal Forfeiture

(a)(1) The court, in imposing sentence on a person convicted of an offense in violation of section 1956, 1957, or 1960 of this title, shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property.

III. Subject Property

This Notice of Demand for Forfeiture includes, but is not limited, to the following:

Money Judgment:

A sum of money that represents the property involved in and/or the amount of proceeds traceable, directly or indirectly, to the violations set forth in Counts One through Eight for which each Defendant is liable.

Substitute Assets:

If any of the property described above, as a result of any act or omission of Defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third person;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States to seek the forfeiture of any other property owned by Defendants up to the value of said Money Judgment as substitute assets, pursuant to FED. R. CRIM. P. 32.2 and 21 U.S.C. § 853(p).

A TRUE BILL

FOREPERSON

GUSTAV W. EYLER
Director, Consumer Protection Branch
United States Department of Justice

JOHN F. BASH
United States Attorney

By: 

EHREN REYNOLDS
YOLANDA MCCRAY JONES
Trial Attorneys

By: 

JOSEPH BLACKWELL
Assistant United States Attorney